What is claimed is:

1. A computer-based method for identifying a situation representing risk to a brokerage or its investors, comprising:

receiving, on a periodic basis, data from at least one source, wherein the data has a first format;

transforming the data from the first format to a second format for analysis;

retrieving an advanced scenario associated with a predetermined activity of one or more individuals, wherein the predetermined activity comprises an undesired behavior relating to securities trading; and

performing detection processing, using the advanced scenario, on a dataset to detect the situation, wherein the dataset includes a portion of the data having the second format, the dataset includes one or more events and entities, and the situation is detected when the detection processing finds at least one instantiation of the undesired behavior.

2. The method of claim 1, wherein the step of performing detection processing includes performing sequence matching to identify sequences in one or more events and relate those sequences to one or more entities in the dataset.

3. The method of claim 1, wherein the step of performing detection processing includes performing link analysis to establish connections between one or more entities and events in the dataset.

4. The method of claim 1, wherein the step of performing detection processing includes performing rule-based analysis to identify at least one of the events and entities based on rules specifying parameters and thresholds for identification of a set of specified events and entities.

5. The method of claim 1, wherein the step of performing detection processing includes performing outlier detection analysis to identify at least one of the events and entities outside of a defined statistical range.

6. The method of claim 1, wherein the step of performing detection processing includes performing decision tree analysis.

7. The method of claim 1, wherein the step of performing detection processing includes using neural networks.

8. The method of claim 1, wherein:

the one or more individuals comprise one or more customers of a securities brokerage;

the activity comprises holding concentrated positions in a single security; and

the dataset includes market value of a concentrated position, and total cash and security value.

9. The method of claim 1, wherein:

the one or more individuals comprise one or more customers of a securities brokerage;

the activity comprises holding a concentrated position in low-priced securities; and

the dataset includes low-priced equities balance, and total cash and security value.

10. The method of claim 1, wherein:

the one or more individuals comprise one or more customers of a securities brokerage;

the activity comprises abusing auto-execution systems; and

the dataset includes order size and order time.

11. The method of claim 1, wherein:

the one or more individuals comprise one or more customers of a securities brokerage;

the activity comprises marking the close;

and the dataset includes order time, holdings by others in a household, and margin maintenance percentage.

12. The method of claim 1, wherein:

the one or more individuals comprise one or more customers of a securities brokerage;

the activity comprises making improper short sales; and

the dataset includes securities sold by an account holder, securities held long by an account holder, and securities purchased by an account holder.

13. The method of claim 1, wherein:

the one or more individuals comprise one or more customers of a securities brokerage;

the activity comprises making cross-trades away from the market; and

the dataset includes execution prices and closing prices.

14. The method of claim 1, wherein:

the one or more individuals comprise one or more customers of a securities brokerage;

the activity comprises behaviors of interest include encouraging orders but marking them as unsolicited; and

the dataset includes number of unsolicited orders and number of solicited orders.

15. The method of claim 1, wherein:

the one or more individuals comprise one or more customers of a securities brokerage;

the activity comprises encouraging short-term holding; and

the dataset includes buy orders, sell orders, and indication of solicitation.

16. The method of claim 1, wherein:

the one or more individuals comprise one or more securities representatives;

the activity comprises soliciting orders but marking them as unsolicited; and

the dataset includes solicitation attempts and unsolicited orders.

17. The method of claim 1, wherein:

the one or more individuals comprise one or more securities representatives;

the activity comprises shadowing a customer's account; and

the dataset includes time between trades in a security.

18. The method of claim 1, wherein:

the one or more individuals comprise one or more brokerage order-takers or employees;

the activity comprises front-running; and

the dataset includes employee account activity and employee-linked account activity.

19. The method of claim 1, wherein:

the one or more individuals comprise one or more brokerage employees;

the activity comprises trading on insider information; and the dataset includes closing prices and trades in an account associated with an employee.

20. The method of claim 1, wherein:

the one or more individuals comprise one or more brokerage employees;

the activity comprises making large deposits; and

the dataset includes employee deposit amounts and employee account net worth.

21. The method of claim 1, wherein:

the one or more individuals comprise one or more customers of a securities brokerage and securities representatives;

the activity comprises rapid switching of mutual funds; and

the dataset includes mutual fund purchase date, mutual fund sale date, and solicitation records.

22. The method of claim 1, wherein:

the one or more individuals comprise an investment advisor;

the activity comprises disproportionate allocation of IPO shares; and

the dataset includes IPO initial trading price, IPO closing price, and subaccount IPO allocation.

23. The method of claim 1, wherein:

the one or more individuals comprise an investment advisor;

the activity comprises unfair allocation of block trades to subaccounts of the investment advisor; and

the dataset includes block trade purchase price, block trade allocation, and security price at time of allocation.

24. The method of claim 1, wherein:

the one or more individuals comprise an investment advisor;

the activity comprises maintenance of concentrated positions in a subaccount of the investment advisor; and

the dataset includes value of individual equities within the subaccount, value of the subaccount, and total number of subaccounts managed by the advisor.

25. The method of claim 1, further comprising generating one or more alerts based on one or more of the found instantiations of the undesired behavior.

26. The method of claim 1, further comprising:

prioritizing the one or more found instantiations of undesired behaviors, wherein the prioritizing is based on user defined logic and values; and

generating one or more alerts based on one or more of the prioritized instantiations of the undesired behavior.

27. The method of claim 1, further comprising:

grouping the one or more found instantiations of undesired behavior, wherein the grouping is based on focus and user defined logic; and

generating one or more alerts based on one or more of the prioritized instantiations of the undesired behavior.

28. The method of claim 27, further comprising prioritizing the groups, wherein the prioritizing is based on user defined logic and values.

29. A method of identifying, using a computer system, an undesired behavior relating to securities trading, comprising:

receiving, on a periodic basis, data having a first format;

transforming the data from the first format to a second format;

selecting a dataset from the data having the second format, wherein the dataset includes one or more events relating to securities trading and one or more entities involved in securities trading;

applying an advanced scenario to the events and entities in the dataset to detect an undesired behavior by one or more of the entities; and

generating an alert when the undesired behavior is detected.

30. The method of claim 29, wherein the applying step comprises using one or more of sequence matching, link analysis, rule-based analysis, outlier detection analysis and decision tree analysis.

31. The method of claim 29, wherein the applying step further comprises prioritizing the detected undesired behavior, and the generating step only generates an alert if an undesired behavior having a predetermined priority is identified.

32. A computer program embodied on a computer readable medium for identifying a situation representing risk to a brokerage or its investors, wherein the program comprises one or more sequences of instructions that cause one or more processors to perform the steps of:

receiving, on a periodic basis, data from at least one source, wherein the data has a first format;

transforming the data from the first format to a second format for subsequent analysis;

retrieving an advanced scenario associated with a predetermined activity of one of more individuals, wherein the predetermined activity comprises an undesired behavior relating to securities trading; and

performing detection processing, using the advanced scenario, on a dataset to detect the situation, wherein the dataset includes a portion of the data having the second format, the dataset includes one or more events and entities, and the situation is detected when the detection processing finds at least one instantiation of the undesired behavior.

33. The computer program of claim 32, wherein the instructions further cause the one or more processors to generate one or more alerts based on detection of the undesired behavior.

34. The computer program of claim 32, wherein the instructions further cause the one or more processors to:

prioritize the undesired behaviors found, wherein the prioritizing is based on user defined logic and values; and

produce one or more prioritized alerts.

35. The computer program of claim 32, wherein the instructions further cause the one or more processors to:

group the undesired behaviors found, wherein the grouping is based on focus and user defined logic; and

produce one or more alerts based on the grouping.

36. The computer program of claim 32, wherein the instructions that cause the detection processing cause the one or more processors to permit an administrator to adjust the time at which detection processing occurs.

37. The computer program of claim 32, wherein the instructions that cause the detection processing cause the one or more processors to permit an administrator to adjust the frequency at which detection processing occurs.

38. The computer program of claim 32, wherein the instructions that cause the detection processing cause the one or more processors to permit an administrator to modify parameters of the advanced scenario.

39. The computer program of claim 32, wherein the instructions that cause the detection processing cause the one or more processors to permit an administrator to request retrieval of additional scenarios.

40. The computer program of claim 32, wherein the instructions that cause the detection processing cause the one or more processors to permit an administrator to remove scenarios.

41. The computer program of claim 32, wherein:

the instructions that cause the detection processing cause the one or more processors to permit an administrator to assign a trust level to focal entities; and

wherein focal entities with a minimum trust level are excluded from alerts.